Nro. Alerta:	AL-2025-048	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	29-ago-2025	Vulnerabilidad Zero-Day — Google Chrome	Pág.: **1** of **3**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad Zero-Day
Tipo de Incidente: Ejecución remota de código / Explotación activa
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Vulnerabilidad Zero-Day — Google Chrome - figura referencial

El equipo Threat Analysis Group de Google reporta una vulnerabilidad Zero-Day definida como CVE-2025-5419, esta falla se encuentra en el motor V8 de JavaScript de Google Chrome que permite ejecución remota de código (RCE). Google ha lanzado una actualización de emergencia.

III. INTRODUCCIÓN

V8 es el motor de JavaScript de código abierto que Google Chrome y otros navegadores basados en Chromium (como Edge, Opera, Brave) utilizan para ejecutar el código JavaScript de las páginas web, incluye también características de seguridad como el espacio V8 Sandbox, que aísla la ejecución de código y protege contra ataques cibernéticos.

IV. VECTOR DE ATAQUE

La explotación de CVE-2025-5419 es un fallo en la lectura/escritura fuera de los límites del motor V8, lo que permite a atacantes remotos corromper la memoria por medio de

páginas web maliciosamente diseñadas, ejecutar código arbitrario e incluso escapar del sandox de Chrome.

Su acceso inicial o ataque se origina en cualquier sitio o contenido web que contenga JavaScript o WebAssembly malicioso.

CVSS:3.1 define el vector de ataque de tipo RED, con una severidad: 8.8 Alta.

V. IMPACTO

Los productos y versiones afectados son los siguientes:

Sistema Operativo / Navegador	Versión Afectada	Estado del Parche
Linux	≤ 137.0.7151.67	Parche disponible: 137.0.7151.68
MacOS	≤ 137.0.7151.67	Parche disponible: 137.0.7151.68
Windows	≤ 137.0.7151.68	Parche disponible: 137.0.7151.69
Microsoft Edge (Chromium)	Versiones heredadas	Actualización pendiente según canal estable
Brave	Versiones heredadas	Actualización pendiente según proveedor
Opera	Versiones heredadas	Actualización pendiente según proveedor
Vivaldi	Versiones heredadas	Actualización pendiente según proveedor

Tabla 1.- Productos y Versiones afectadas - Vulnerabilidad Zero-Day — Google Chrome

- Ejecución de código no autorizado mediante la carga de sitios web especialmente diseñados.
- Posibilidad de extraer o manipular datos al aprovechar navegadores que no han sido actualizados.
- Riesgo de comprometer sistemas internos a través de accesos iniciales desde entornos web vulnerables**.**

VI. INDICADORES DE COMPROMISO

- Cualquier sitio o contenido web que contenga Javascript o WebAssembly malicioso.
- Chrome v137.0.7151.68/.69 o cualquier navegador basado en Chromium.

VII. RECOMENDACIONES:

- Actualizar Google Chrome a la versión 137.0.7151.68/.69 inmediatamente.
- Supervisar el tráfico saliente hacia dominios sospechosos.
- Aplicar control de ejecución de scripts en navegadores.
- Habilitar soluciones EDR para identificar comportamiento anómalo.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

NVD (2025). Detalles sobre CVE-2025-5419. https://nvd.nist.gov/vuln/detail/CVE-2025-5419

RAPID7 (2025). Google Chrome CVE-2025-5419 Vulnerability Analysis. https://www.rapid7.com/db/vulnerabilities/google-chrome-cve-2025-5419/

HELPNETSECURITY (2025). Google soluciona vulnerabilidad Zero-Day explotada activamente en Chrome. https://www.helpnetsecurity.com/2025/06/04/google-fixes-chrome-zero-day-with-in-the-wild-exploit-cve-2025-5419/

SECPOD (2025). Google lanza parche de emergencia para nueva Zero-Day en Chrome. https://www.secpod.com/blog/new-chrome-zero-day-actively-exploited-google-issues-emergency-out-of-band-patch/

CVE DETAILS (2025). Información técnica sobre CVE-2025-5419. https://www.cvedetails.com/cve/CVE-2025-5419/